FORTINET
High Performance Network Security

FortiConnect

Release 16.8

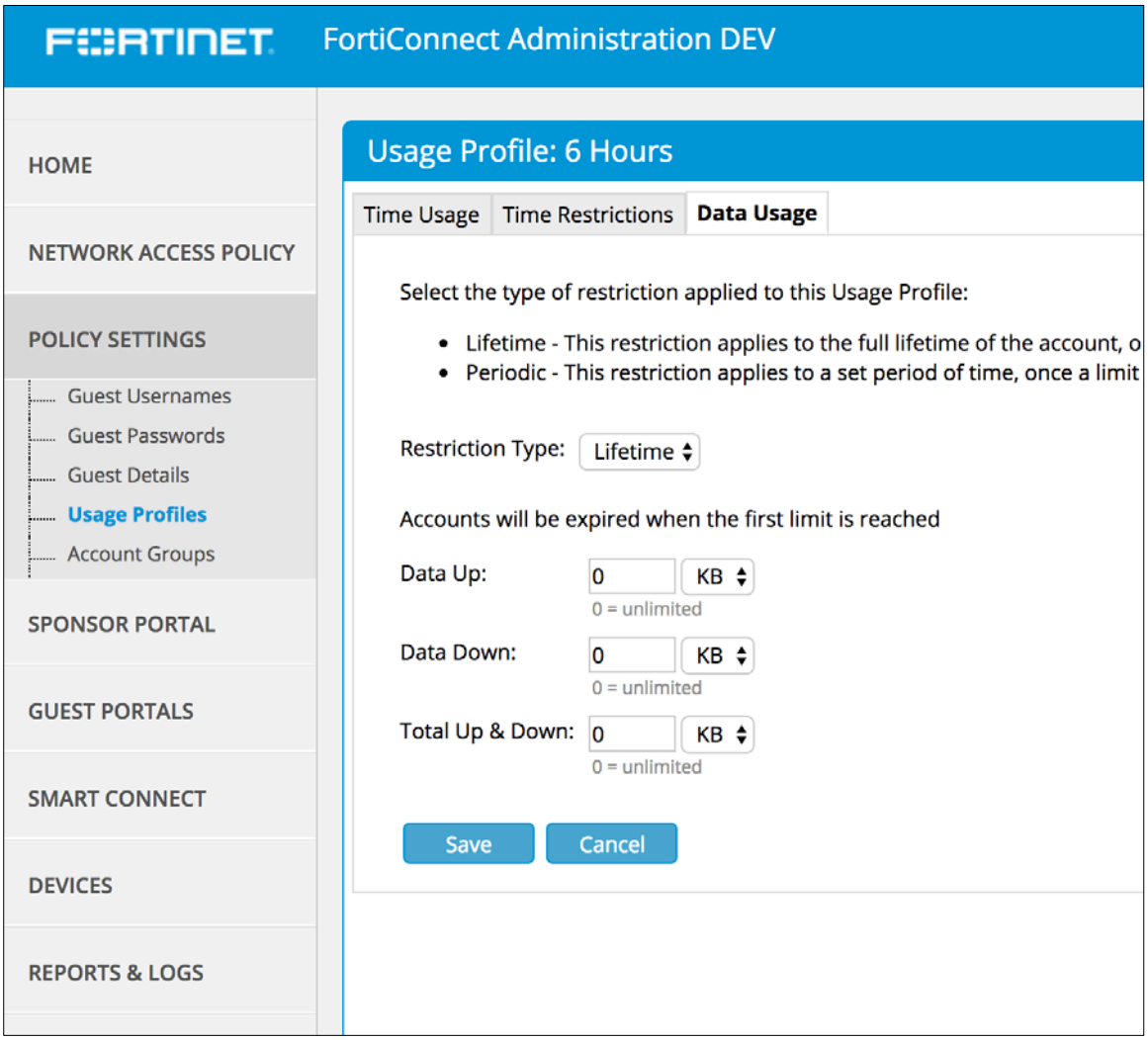
FortiConnect is a complete provisioning, management, and reporting system that provides temporary network access for guests, visitors, contractors, consultants, or customers. FortiConnect works alongside Wireless Controllers, LAN Switches, NAC Systems, Firewalls and other Network Enforcement devices which provide the captive portal and enforcement point for guest access.

This release comes with important fixes and the following new features.

Time Based Data Cap

Administrators can now configure periodic data usage restrictions. By enabling these restrictions, the permitted data usage is available only for the time period specified as Daily, Weekly, or Monthly.

The new options are available at **Policy Settings** > **Usage Profiles** > **Data Usage** Tab.



Support for using CHAP protocol for MAC Based Authentication

Starting with this release, MAC based authentication can use the CHAP protocol.

IP Address are Hidden from Redirect URLs

Redirect URLs can be configured to hide IP address. Supported URLs format/slugs are:

- /portal/<device ip>
- /portal/UniFi
- /portal/detect
- /portal/<portal name>/<device ip>
- /portal/<portal name>/detect
- /portal/<portal name>/preview
- /portal/source/<device name>
- /portal/<portal name>/source/<device name>

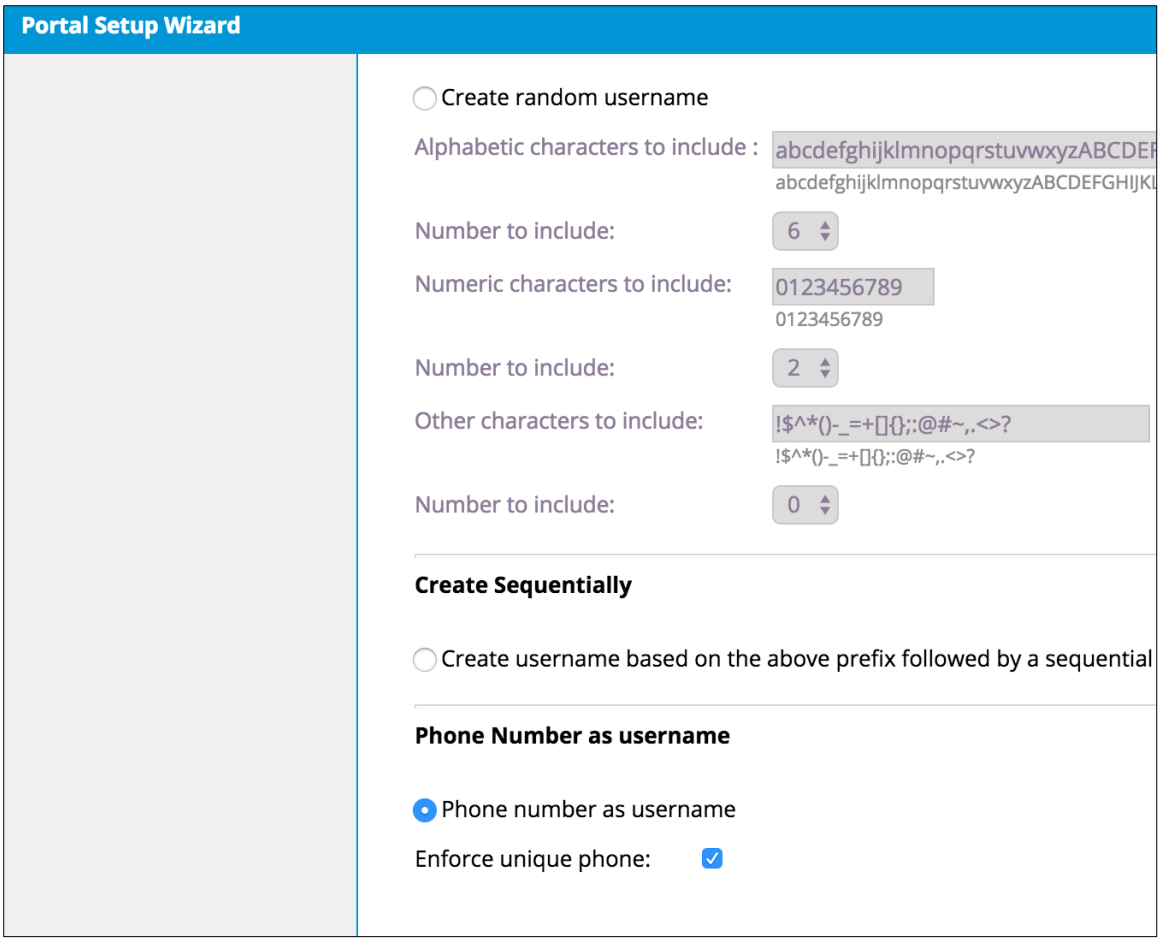
Support for non-US based Authorize.net payment processor accounts

Starting with this release, your customers can use non-US based Authorize.net payment processor accounts.

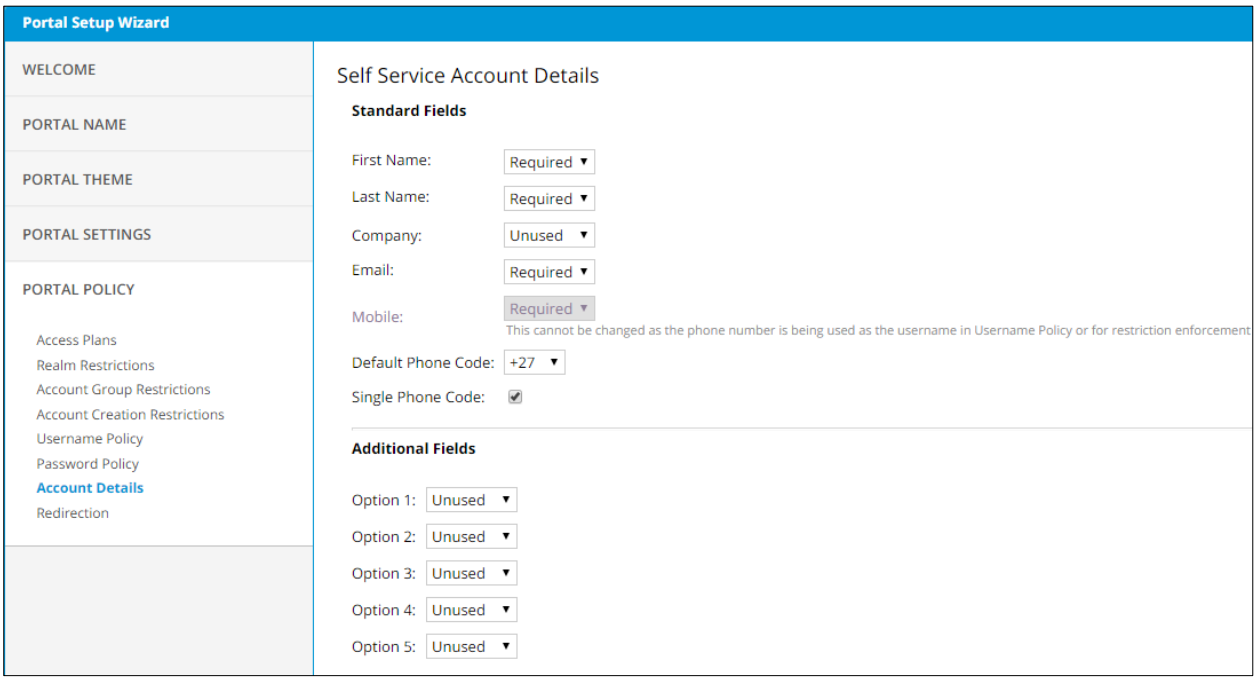
Support for Registration via Mobile Phone Number and SMS

Users can now use their mobile phone number to register in the guest portal. When a phone number is used for registration, a randomly generated password is sent to the user via SMS.

A new option “Phone number as Username” is added to the Policy Setup Wizard.



NOTE: Select 'Enforce Unique Phone' to ensure that only one account is active with the given phone number. If this option is unselected then a new account is created but a number is appended to the end of the phone number.



Select the **Single Phone Code** option in Account details page to enforce the default selected phone code to be used as country code while generating the account.

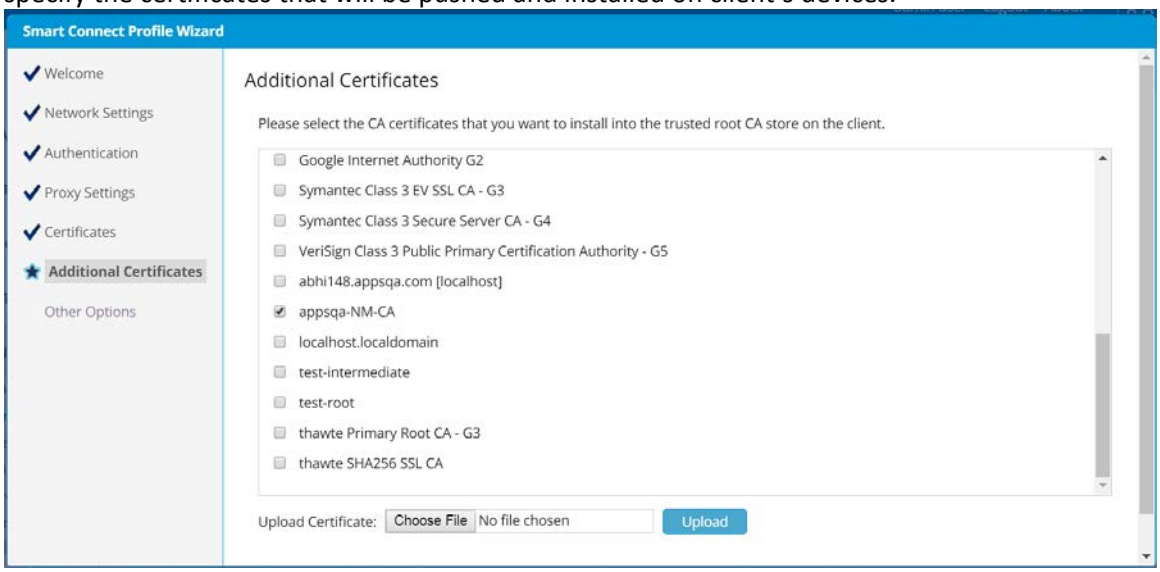
Enhanced Android On boarding

By integrating with SD, you can set up SmartConnect portal without a static whitelist to open access to the Google Play store.

Ability to Push and Install Certificates to Clients

You can now specify additional certificates that are used for other purposes then securing the 802.1X connection, as part of the SmartConnect profile. This will then be installed on the client and placed in the relevant trusted certificate store.

A new page *Additional Certificates* is available in the SmartConnect Profile Wizard that allows you to specify the certificates that will be pushed and installed on client's devices.



Note: Supported on Android devices running on version 7.0 or newer and requires users to accept certificate installation. SmartConnect on Linux OS does not support this feature.

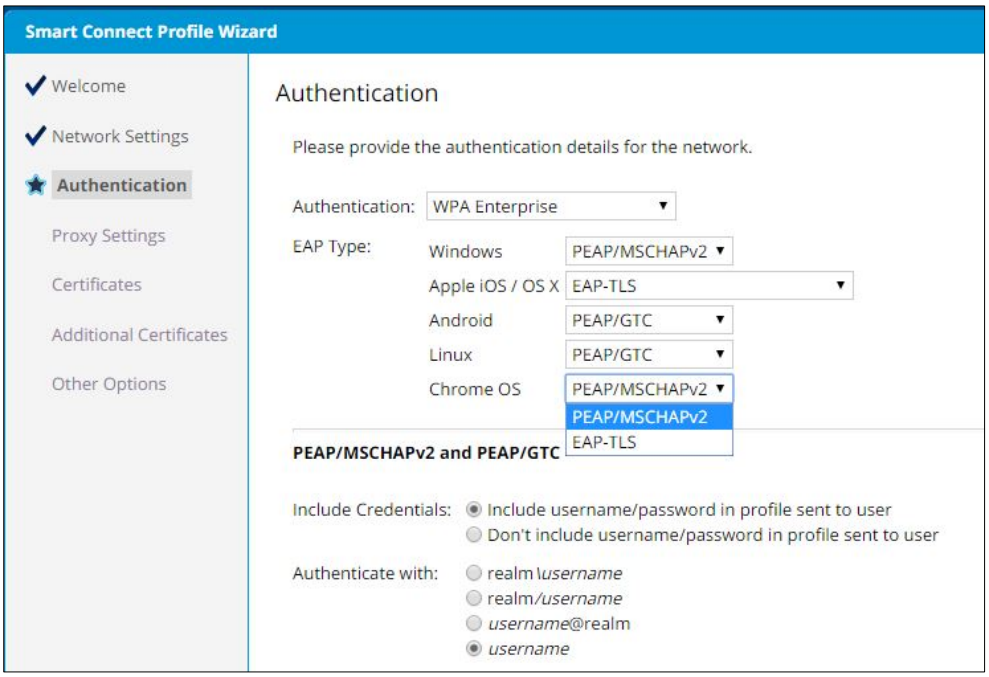
Extend Network Usage using Same Credentials

Users can now easily extend their network usage by purchasing additional usage credits using their existing credentials. To provide this functionality to your users, enable **Post Authentication** option for *My Account* and *Credit Card Billing* in the Portal Pages page of the Portal Setup Wizard (Guest Portal > Portal Setup Wizard > Portal Settings > Portal Pages > My Account).

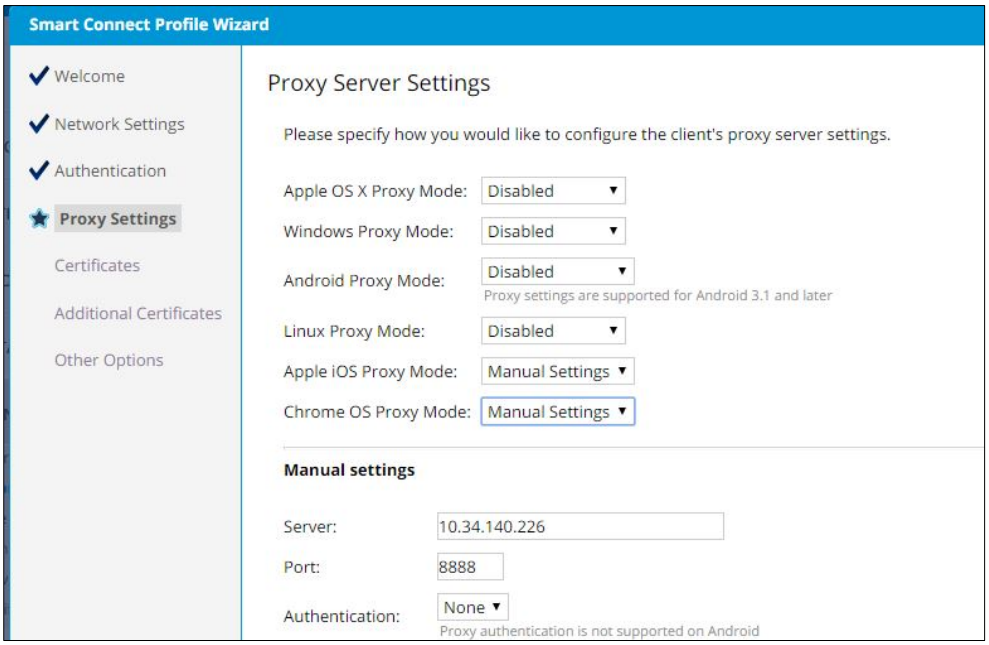
Support for Google Chromebooks

Google Chromebook users can now connect to secure network using SmartConnect profile.

Select EAP type at the SmartConnect Profile Wizard > Authentication page.



Configure Proxy Settings at SmartConnect Profile Wizard > Proxy Settings page.



NOTE: Proxy authentication is not supported in Chromebooks.

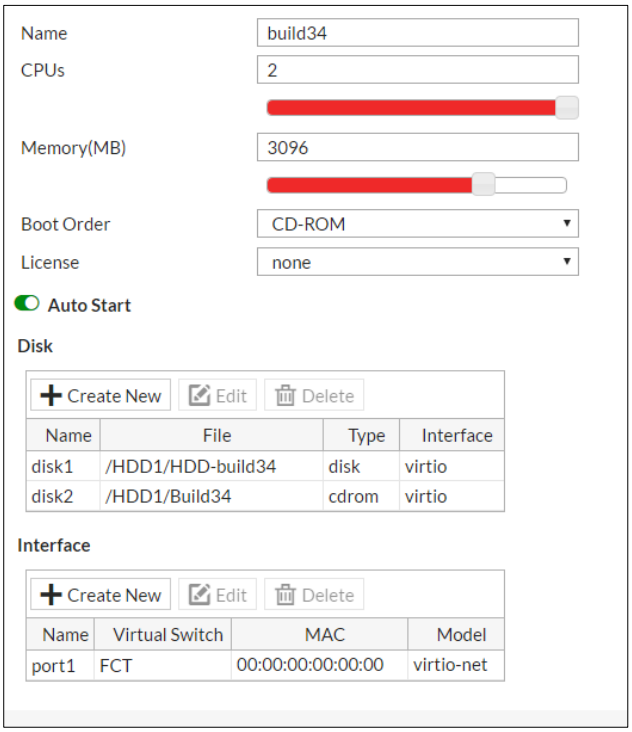
Steps to connect using SmartConnect profile

1. After CP authentication, users are redirected to SmartConnect download page. Click the Download button to get the ONC file.
2. In the browser, go to **chrome://net-internals/#chromeos** URL and select the ONC file downloaded in the previous step and then click the **IMPORT** button.
3. Once the import is complete, the SmartConnect profile is displayed in the preferred list.

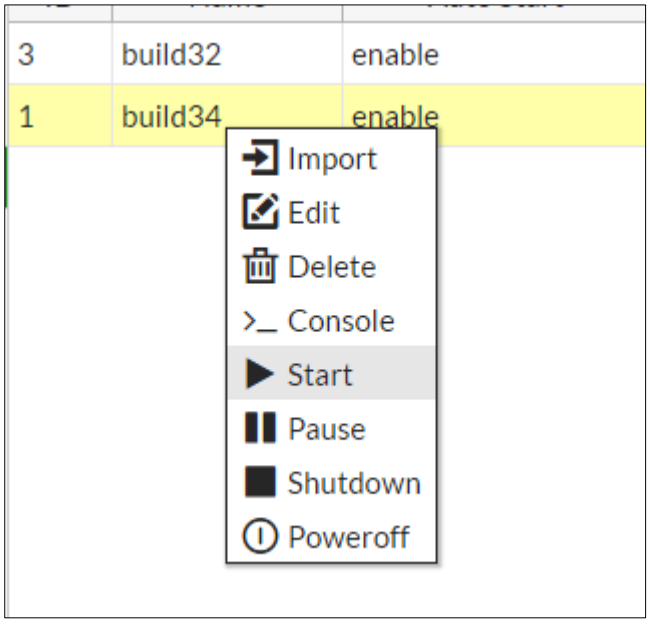
FortiConnect Support in FortiHypervisor

Use the following steps to install FortiConnect in a FortiHypervisor.

1. Go to Image and click Upload button to FortiConnect image file.
2. Go to Image and click the Create New button to create a harddisk
3. Go to Virtual Machine and click Create New button to set up a new virtual machine for Smart Connect. In this VM, set boot order to CD-ROM.
4. Select disks, the image file and interface settings.



5. Click Virtual Machine, then right click the newly created VM and click the Start button.



6. Right click the newly created VM and select Console. This will open a console window in a new tab. Type **FHY** to install FortiConnect in Hypervisor.
7. During the installatoin process after the reboot, change the bootorder (refer step-3) to harddisk.

List of Known Issues

BUGId	Descriptoin
0413075	User is unable to connect secure network without entering password.
0415919	Wired authentication is not stable in chrome books and SmartConnect is not displayed in preferred list for wired profiles
0416095	Installing FCT in FortiHypervisor requires manual change of boot order from CDROM to HDD,
0416098	In FortiHypervisor setup, the shutdown option is not working for FCT instance.
0417633	Screen interface is busy/frozen after downloading CSV files from sponsor portal.

Additional Resources

In addition to the release notes, the following documentation is available.

- FortiConnect User Guide
- FortiWLC (SD) Configuration Guide

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Support and Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service